# Information Security Standard – System Integrity

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the system integrity controls to be implemented across all of {Company}’s systems.

## Applicability

Compliance with the controls outlined in this document is mandatory for all {Company} employees, contractors, vendors, and guests.

## Non-compliance

Any instances of non-compliance with the controls outlined in this document should be reported following the procedures outlined in the Reporting Process.

## Scope

The requirements of this standard to all systems that store, process, or transmit {Company} information; or are used to connect to those systems that are used to store, process, or transmit {Company}’s information.

## Controls

1. All changes to the production system, including third-party patches, must first be tested in a non-production environment before being deployed. These tests must validate the efficacy of the proposed change, as well as validate that any side-effects of the changes are known and acceptable.
2. All known issues in the {Company} platform must be tracked and assigned a ticket in {Company}’s JIRA instance.
3. Any patches or fixes for security vulnerabilities must be deployed to production according to the following schedule:

|  |  |
| --- | --- |
| **Risk Rating** | **Timeframe after release by engineering or third-party.** |
| Critical | Within 7 days whenever possible, but no longer than 30 days |
| High | 30 Days |
| Moderate or Medium | 60 Days |
| Low | 90 Days |

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.0 |
| Date Modified | 30 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |